EXHIBIT "1"

SUPREME COURT STATE OF NEW YORK
COUNTY OF NEW YORK

---x

BANCO DEL AUSTRO, S.A. Index#:

Plaintiff,

-against-

WELLS FARGO BANK, N.A.

Defendant.

---x

COMPLAINT

1. Banco del Austro, S.A. ("BDA"), sues Wells Fargo Bank, N.A. ("WFB"), for breaches of contractual, statutory and common law duties related to unauthorized debits from BDA's correspondent account maintained at WFB, and states:

PARTIES, JURISDICTION AND VENUE

2. Plaintiff BDA is a foreign bank incorporated and organized under the laws of Ecuador.
3. Defendant WFB is a national banking association organized and existing under the laws of the United States, with its head office in San Francisco, California, and its registered office in Sioux Falls, South Dakota.
4. Pursuant to the agreement between BDA and WFB entitled "Terms and Conditions for Global Financial Institutions" (the "Agreement"), the parties agreed that any legal proceeding against WFB may be

commenced in the courts of the Borough of Manhattan, New York City, in the State of New York. Agreement ¶ 7.9.

5. This Court thus has personal jurisdiction over WFB because WFB consented to be sued in the courts of the Borough of Manhattan, New York City, in the State of New York pursuant to paragraph 7.9 of the Agreement.

6. In addition, venue is proper in New York County, New York, because WFB consented to the forum selection clause in paragraph 7.9 of the Agreement, and BDA designates New York City in the State of New York as the venue in this action.

FACTS

Correspondent Account Relationship between BDA and WFB

7. BDA has no branches in the United States.

8. Accordingly, BDA needed a correspondent banking relationship with a United States-based bank to conduct international banking operations, including funding overseas payments and wiring transfers requested by its clients in Ecuador.

9. As a result, BDA and WFB commenced a correspondent banking relationship that led to the establishment of BDA's correspondent account with WFB (hereinafter, the "Correspondent Account").

10. The correspondent banking relationship was governed in part by Wells Fargo Bank, N.A.'s Terms and Conditions for Global Financial

Institutions, which was executed in February 2011 (hereinafter, the "Agreement," a true and correct copy of which is attached hereto as Exhibit "A").

11. The terms of the Agreement consisted of BDA agreeing to pay correspondent banking fees to WFB, and WFB agreeing to service BDA's Correspondent Account, perform transactions properly authorized by BDA, and safeguard the property of BDA's Correspondent Account by complying with various laws of the United States and general US commercial banking practices, including implementing a program for fraud detection, and reporting to BDA any unusual or suspicious activity impacting BDA's Correspondent Account.

12. Indeed, WFB assured BDA that not only would the relationship be also governed by the laws of the State of New York, including Article 4A of the Uniform Commercial Code, but also that WFB would comply with all Laws of the United States applicable to it, including the USA PATRIOT ACT, and general US commercial banking practices. Agreement ¶¶ 7.7 and 7.8.

13. As part and parcel of such commitment, WFB acknowledged that WFB's compliance with Laws to which it is subject may affect the transactions BDA may conduct with, or through, WFB and may require that BDA provide or certify information to WFB about itself or any entity or class of entities transacting payments or other business through BDA's

Correspondent Account or through BDA's use of other services. Agreement ¶ 7.8.

14. On July 31, 2014, WFB further boasted to BDA that WFB, through its financial crimes risk management program ("Global FCRM Program") designed to comply with the various laws of the United States[1], had detective controls, which included identifying unusual activity; automated transaction monitoring; customer surveillance; investigating the unusual activities identified, and determining whether they are suspicious; monitoring customer activity, and applying predictive analytics for customer-centric, cross-channel fraud detection; screening, blocking, and rejecting transactions appropriately; and reporting these matters (along with other regulatory reporting requirements).

15. Accordingly, WFB assured BDA that WFB had security policies and procedures in place necessary to detect and deter suspicious or fraudulent activity and to report them to BDA (along with other regulatory reporting requirements), which reporting would alert BDA of such anomalous activity, and allow BDA to prevent the fraud.

16. Based on WFB's assurances, BDA reasonably expected to be alerted by WFB if WFB observed or should have observed any suspicious activity,

---

[1] WFB specifically represented that, through its Global FCRM Program, it managed ***financial crimes*** risks associated with Bank Secrecy Act ("BSA"), Anti-Money Laundering ("AML"), ***External Fraud***, and other laws.

which had the potential to materially impact BDA's Correspondent Account.

17. Indeed, consistent with general US commercial bank practices, like the ones represented by WFB, BDA reasonably expected to be alerted by WFB if the Correspondent Account experienced any unusual activity, and to have WFB block any anomalous activity.

18. Pursuant to the terms of the Agreement, BDA would generate the wire transfers using the Society for Worldwide Interbank Financial Telecommunications ("SWIFT") network, which must be accessed from within BDA's computer system.

19. The Agreement further provided that for SWIFT messages, the SWIFT Authentication procedures with the SWIFT User Handbook would be used as the Security Procedure to verify that BDA was the originator of a payment order. Agreement ¶ 3.1.

20. However, although the SWIFT Authentication procedure would be used to verify whether BDA was the originator of a payment order, (Agreement ¶ 3.1), it could not be used to verify whether suspicious activity originating from BDA's SWIFT terminal was fraudulent (due to third-party hacking, as happened in this case) or in fact authorized by BDA (as both would show as "originating" from BDA).

21. BDA reasonably expected that, based on WFB's own material representations, such fraud detection would be done by WFB using its detective controls pursuant to WFB's Global FCRM Program.

Suspicious Activity in the Account (the Unauthorized Transfers)

22. On January 21, 2015, BDA reported to WFB that unauthorized debits from the Correspondent Account were made by WFB, and that those unauthorized debits were determined to be fraudulent transactions.

23. As a result of the fraudulent transactions, on January 21, 2015, BDA issued fraud alerts through SWIFT to WFB for the unauthorized transfers which are detailed below (collectively, they shall hereinafter be referred to as the "Unauthorized Transfers"):

	Date	Time	Sender	Amount (US$)	Beneficiary	Beneficiary's Bank	City
1.	1/12/2015	7:24 pm	Marina Breeze	$986,256.88	Mester Trading Corp.	HSBC	Hong Kong
2.	1/12/2015	7:02 pm	Femar	$1,424,638.06	Regal Prosper Trading Limited	HSBC	Hong Kong
3.	1/13/2015	7:04 pm	Constrin dec, S.A.	$1,236,578.45	Regal Prosper Trading Limited	HSBC	Hong Kong
4.	1/13/2015	9:16 pm	Econotra ns Ecuador	$663,297.31	Regal Prosper Trading Limited	HSBC	Hong Kong

5.	1/13/2015	10:38 pm	Econotrans Ecuador	$96,325.23	Nectali Martinez Hernandez	JP Morgan Chase	New York
6.	1/14/2015	12:01 am	Audiolec	$1,485,230.89	Regal Prosper Trading Limited	HSBC	Hong Kong
7.	1/14/2015	11:51 pm	Constrindec, S.A.	$1,375,240.23	Regal Prosper Trading Limited	HSBC	Hong Kong
8.	1/14/2015	7:06 pm	Audiolec	$1,486,230.22	Jose Mariano Castillo	Wells Fargo	L.A.
9.	1/16/2015	6:29 pm	Cosmica	$1,056,780.56	Fratelli Investments Limited	Mashrebank PSC	Dubai
10.	1/20,2015	6:56 pm	Indisir	$298,223.15	No Beneficiary Identified	HSBC	Hong Kong
11.	1/20/2015	11:46 pm	Raslogec	$95,731.18	JGM Asia Telecom	Hang Seng Bank	Hong Kong
12.	1/21/2015	7:56 pm	Autoline	$1,968,230.25	Jiushun Group Co.	HSBC	Hong Kong
			TOTAL:	$12,172,762.41			

24. True and correct copies of the Unauthorized Transfers are attached as Exhibit "B" hereto.

25. A routine manual and/or automated comparison of each of the Unauthorized Transfers to the normal activity in the Correspondent

Account would have flagged each of them as unusual or unexpected, and thus indicative of fraud.

26. Indeed, some or all of the Unauthorized Transfers exhibited the following unusual or anomalous characteristics:

    a. Unusual times of day for the SWIFTs (given that all were outside normal operating hours of BDA's SWIFT);

    b. Unusual amounts;

    c. Unusual beneficiaries in unusual geographic locations (ten out of the twelve transfers were to beneficiaries located in Hong Kong and Dubai);

    d. Unusual frequency of transfer (twelve in nine days, with the second, third and fourth transfers being to the same entity in Hong Kong within the span of a mere two days for substantial sums of money); and

    e. The same beneficiary receiving funds from multiple originators (e.g., Regal Prosper Trading Limited receiving funds from three different customers of BDA).

27. In sum, the Unauthorized Transfers were made in unusual times of the day, in unusual amounts, to unusual beneficiaries in unusual geographic locations (ten of twelve, including the first four), and in an unusual frequencies. For example, three of the first four wires, in the amounts of $1,424,638.06, $1,236,578.45 and $663,297.31, were created outside the

normal operating business hours of BDA and its SWIFT system, were in high amounts, sent to the **same** entity ("Regal Prosper Trading Limited") in an unusual geographic location (Hong Kong), within the span of only two days (January 12 and 13, 2015), from **three** different customers of BDA.

28. In addition, although the twelfth Unauthorized Transfer for $1,968,230.25 was made after business hours at 7:56 pm on January 21, 2015, WFB processed the Unauthorized Transfer despite BDA's alerting WFB of the fraudulent nature of the transaction a mere three hours after the Unauthorized Transfer's SWIFT message was sent.

29. Despite the numerous anomalies in the Unauthorized Transfers, WFB inexplicably failed to block them and/or alert BDA of the suspicious activity.

30. Had WFB, at a minimum, notified BDA of the suspicious activity, the loss would have been avoided, inasmuch as BDA would have notified WFB in response that the suspicious activity was in fact fraudulent.

31. Indeed, on January 21, 2015, after conducting a regular audit of the Correspondent Account, BDA discovered the Unauthorized Transfers. BDA discovered that for each Unauthorized Transfer, an unauthorized user remotely accessed BDA's computer system after hours, logged onto the SWIFT network purporting to be BDA, and redirected transactions to new beneficiaries with significant dollar amounts.

32. Upon discovery of the fraud, BDA promptly informed its correspondent banks, including WFB, that received unauthorized transfers about the fraudulent nature of the transactions and sought to have the transactions cancelled and its funds returned.

33. On January 27, 2015, Citibank refunded the sum of US$1,845,286.86 to BDA as a result of the fraud alert issued by BDA as to an unauthorized transfer to its correspondent account maintained at Citibank for the same amount.

34. On February 18, 2015, WFB made a partial refund of the Unauthorized Transfer in the amount of US$1,486,230.22 by refunding the sum of US$958,700.27 to BDA as a result of the fraud alert issued by BDA. Inexplicably, WFB only made a partial refund despite the Unauthorized Transfer being traced to one of its customers.[2]

35. By letter dated April 7, 2015, BDA reiterated its demand to WFB for the immediate refund of the Unauthorized Transfers to BDA's Correspondent Account. A true and correct copy of the letter is attached hereto as Exhibit "C."

36. BDA also initiated proceedings in Hong Kong against various recipients of the Unauthorized Transfers in an effort to recover funds from the

[2] Egregiously, instead of refunding all of the Unauthorized Transfers, as the law requires, WFB notified BDA on February 20, 2015, that it had "ascertained that [the] relationship with Banco del Austro ('BDA', 'you', and 'your') no longer

Unauthorized Transfers. The claims are for unlawful receipt and retention of funds, unjust enrichment and restitution, injunctive relief, and an accounting related to the Unauthorized Transfers.

37. All conditions precedent to this action have occurred, been waived, or excused, or WFB is estopped from asserting the existence of any or all such conditions by its own conduct.

AS AND FOR A FIRST CAUSE OF ACTION
BREACH OF CONTRACTUAL DUTIES

38. Plaintiff BDA incorporates by reference paragraphs 1 to 37 as if fully set forth herein.

39. Under the terms of the Agreement, in return for payment of correspondent banking fees, WFB agreed to verify the authenticity of SWIFT payment orders pursuant to the SWIFT Authentication procedures in accordance with the SWIFT User Handbook, and to act, as to the payment orders, in compliance with all applicable laws and general US commercial bank practices. Agreement ¶¶ 3.1 and 7.7.

40. Pursuant to general banking practices, commercial banks in the United States implement and follow "know your customer" and fraud detection policies and procedures designed to detect and deter suspicious activity in the accounts, and to report such anomalies to, among others, its customers.

---

meets [its] business profile requirements." As a result, WFB closed the

41. Consistent with industry practice, WFB trumpeted to BDA that it implemented and followed its Global FCRM Program as a fraud detection mechanism.

42. According to WFB's assurances, its Global FCRM Program's Second Pillar contained internal controls divided in "preventive" and "detective."

43. Among the "detective" internal controls, WFB boasted to BDA that it included the ability to identify unusual activity in the account, apply predictive analytics for customer-centric, cross-channel fraud detection, screen, block and reject suspicious transactions, and report these matters (along with other regulatory reporting requirements).

44. WFB materially breached its contractual duties by failing to detect, block and report the Unauthorized Transfers.

45. As a direct and proximate result of WFB's material breaches of contract, BDA has suffered damages.

AS AND FOR A SECOND CAUSE OF ACTION
BREACH OF STATUTORY DUTIES

46. Plaintiff BDA incorporates by reference paragraphs 1 to 37 as if fully set forth herein.

47. Section 4-A-204(1) of the Uniform Commercial Code provides in pertinent part that:

Correspondent Account.

> If a receiving bank accepts a payment order issued in the name of its customer as sender which is ... not authorized and not effective as the order of the customer under Section 4-A-202, ...the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund.

48. BDA did not authorize the Unauthorized Transfers.

49. BDA is not otherwise bound to the Unauthorized Transfers by the law of agency, as the Unauthorized Transfers were transmitted electronically via SWIFT.

50. Thus, the Unauthorized Transfers are not enforceable pursuant to Section 4-A-202(1) of the Uniform Commercial Code.

51. The Unauthorized Transfers are also not enforceable pursuant to Section 4-A-202(2) of the Uniform Commercial Code because WFB failed to accept the Unauthorized Transfers in good faith and in compliance with the security procedure agreed-upon in the Agreement.

52. Under the terms of the Agreement, in return for payment of correspondent banking fees, WFB agreed to verify the authenticity of SWIFT payment orders pursuant to the SWIFT Authentication procedures in accordance with the SWIFT User Handbook.

53. The Agreement further protected BDA against the risk of unauthorized payment orders by requiring that WFB act, as to the payment orders, in

compliance with all applicable laws and general US commercial bank practices. Agreement ¶¶ 3.1 and 7.7.

54. Thus, WFB not only had to comply with the SWIFT Authentication procedures, but also with all applicable laws and general US commercial bank practices, including any fraud detection policies and procedures adopted by it and represented to BDA.

55. Pursuant to general banking practices and in compliance with US law, commercial banks in the United States implement and follow "know your customer" and fraud detection policies and procedures designed to detect and deter suspicious activity in the accounts, and to report such anomalies to, among others, its customers.

56. Consistent with industry practice and to comply with US laws, WFB trumpeted to BDA that it implemented and followed its Global FCRM Program as a fraud detection mechanism.

57. According to WFB's assurances, its Global FCRM Program's Second Pillar contained internal controls divided in "preventive" and "detective."

58. Among the "detective" internal controls, WFB boasted to BDA that it included the ability to identify unusual activity in the account, apply predictive analytics for customer-centric, cross-channel fraud detection,

screen, block and reject suspicious transactions, and report these matters (along with other regulatory reporting requirements).[3]

59. WFB failed to detect, block and report the Unauthorized Transfers under its Global FCRM Program.

60. In doing so, WFB failed to properly follow the security procedure, with the limitations in place designed to further protect BDA.

61. In addition, WFB failed to accept the Unauthorized Transfers in good faith because it failed to observe reasonable commercial standards of fair dealing.

62. Specifically, WFB failed to comply with its own fraud detection policies and procedures, which it trumpeted to BDA. It failed to detect, block and report to BDA the Unauthorized Transfers, despite their various unusual or anomalous characteristics.

63. In view of the various anomalies and unusual activity related to the Unauthorized Transfers, WFB's failure to detect, block and report to BDA the Unauthorized Transfers demonstrates a lack of good faith.

64. As a result, section 4-A-204(1) of the Uniform Commercial Code requires that WFB refund the Unauthorized Transfers (minus any amounts already refunded), plus interest.

---

[3] Thus, WFB boasted that its Global FCRM Program was "customer-centric." In effect, WFB represented that its Global FCRM Program was customized to meet the circumstances of the particular customer, including its size, type and frequency of payment orders (i.e., normal account activity).

65. To date, WFB has failed to comply with section 4-A-204(1) by refusing to refund the Unauthorized Transfers (minus the amount already refunded) to BDA.

66. As a direct and proximate result of WFB's breaches of its statutory duty, BDA has suffered damages.

AS AND FOR A THIRD CAUSE OF ACTION
BREACH OF COMMON LAW DUTIES

67. Plaintiff BDA incorporates by reference paragraphs 1 to 10, 14 to 18, and 21 to 37 as if fully set forth herein.

68. BDA was entitled to the protections afforded by law to customers of financial institutions.

69. Under the law, WFB owed BDA a duty of care independent of the Agreement.

70. WFB had an independent duty of care in providing correspondent banking services to BDA in a manner consistent with reasonable industry standards, including the implementation and proper execution of adequate "know your customer" and fraud detection policies and procedures, as trumpeted by WFB.

71. Consistent with reasonable industry standards, WFB's duty of care required that it implement and follow "know your customer" and fraud detection policies and procedures designed to monitor for suspicious activity in the Correspondent Account, screen, block, and reject

anomalous transactions in the Correspondent Account, and report those anomalous transactions in a timely manner to BDA.

72. Under the circumstances, WFB violated its duty of care by negligently honoring the Unauthorized Transfers, and thereby negligently failing to properly monitor the Correspondent Account for suspicious activity, failing to screen, block and reject the Unauthorized Transfers, and/or failing to report the Unauthorized Transfers in a timely manner to BDA.

73. Each Unauthorized Transfer should have triggered an alert at WFB pursuant to proper "know your customer" and fraud detection policies and procedures in place. WFB should have recognized and blocked the Unauthorized Transfers as suspicious and anomalous, given the expected and actual activity in the Correspondent Account.

74. This recognition should have then triggered a reporting process that would have notified BDA of the Unauthorized Transfers.

75. Such a simple reporting process would have revealed the scheme by outsiders and averted the losses resulting from the Unauthorized Transfers, as BDA would have verified that any of the transactions at issue was unauthorized.

76. As a direct and proximate result of WFB's negligence, BDA suffered damages.

WHEREFORE, the Plaintiff respectfully demands judgment against the Defendant on the First, Second, and Third Causes of Action for compensatory damages, plus costs, interest, and attorney's fees, together with all other and further such relief that the Court may deem just and necessary.

Dated: January 7, 2016

/s/ John G. Marfoe
John G. Marfoe, Esq.
WNF Law, P.L.
Attorneys for Plaintiff
1111 Brickell Ave., Suite 2200
Miami, Florida 33131